Fig.1a.

EXAMPLE OF VIRUS CHANGING PROGRAM ENTRY POINT

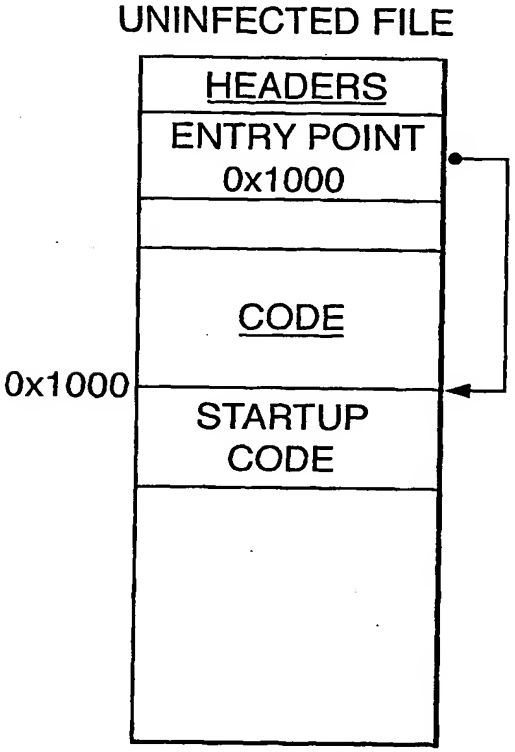


Fig.1b.

EXAMPLE OF VIRUS CHANGING PROGRAM ENTRY POINT

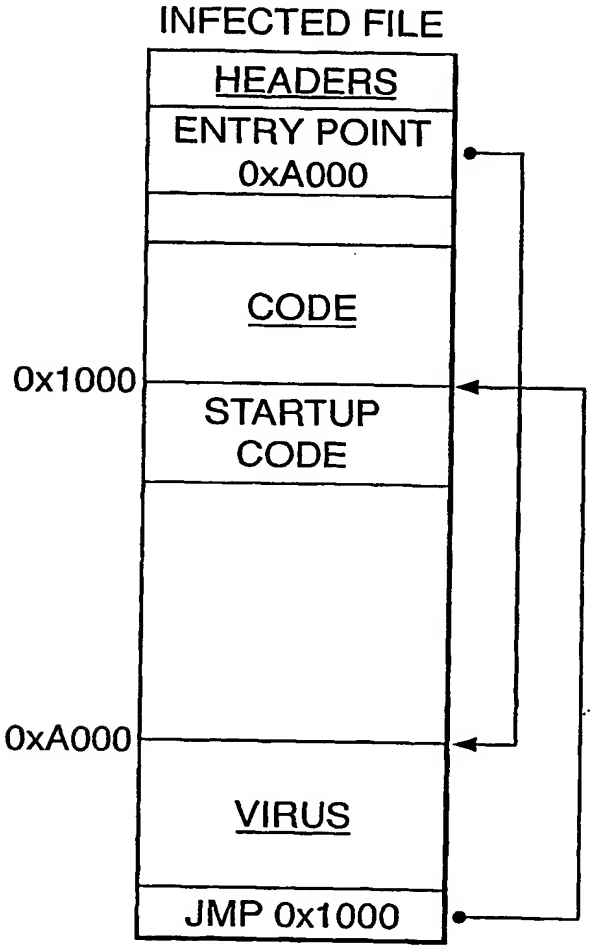


Fig.2a.

EXAMPLE OF VIRUS OVERWRITING CODE AT PROGRAM ENTRY POINT

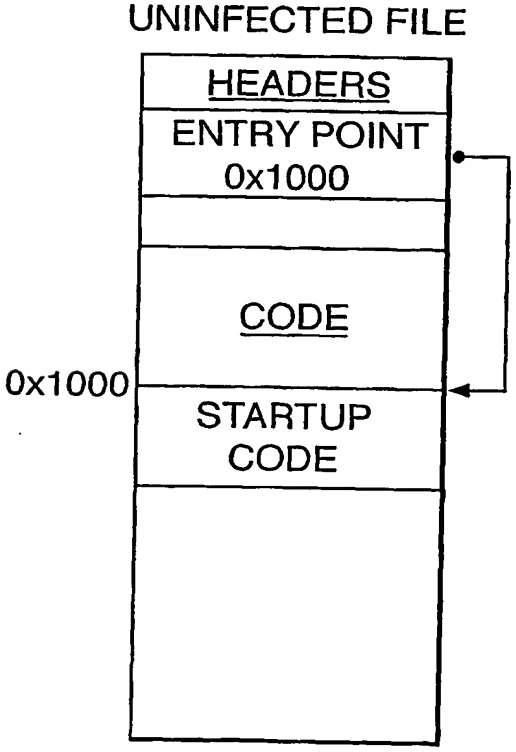


Fig.2b.

EXAMPLE OF VIRUS OVERWRITING CODE AT PROGRAM ENTRY POINT

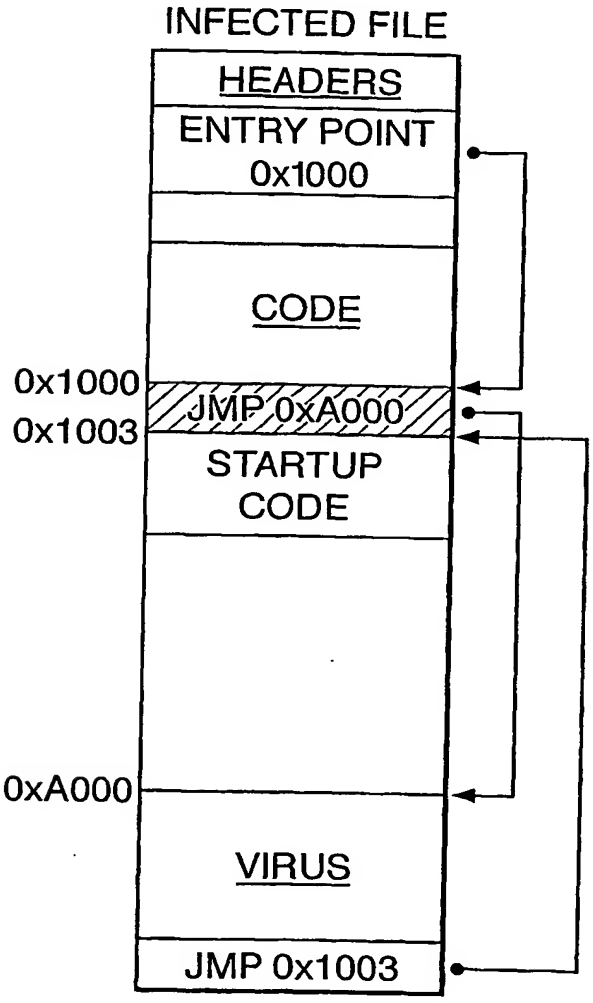
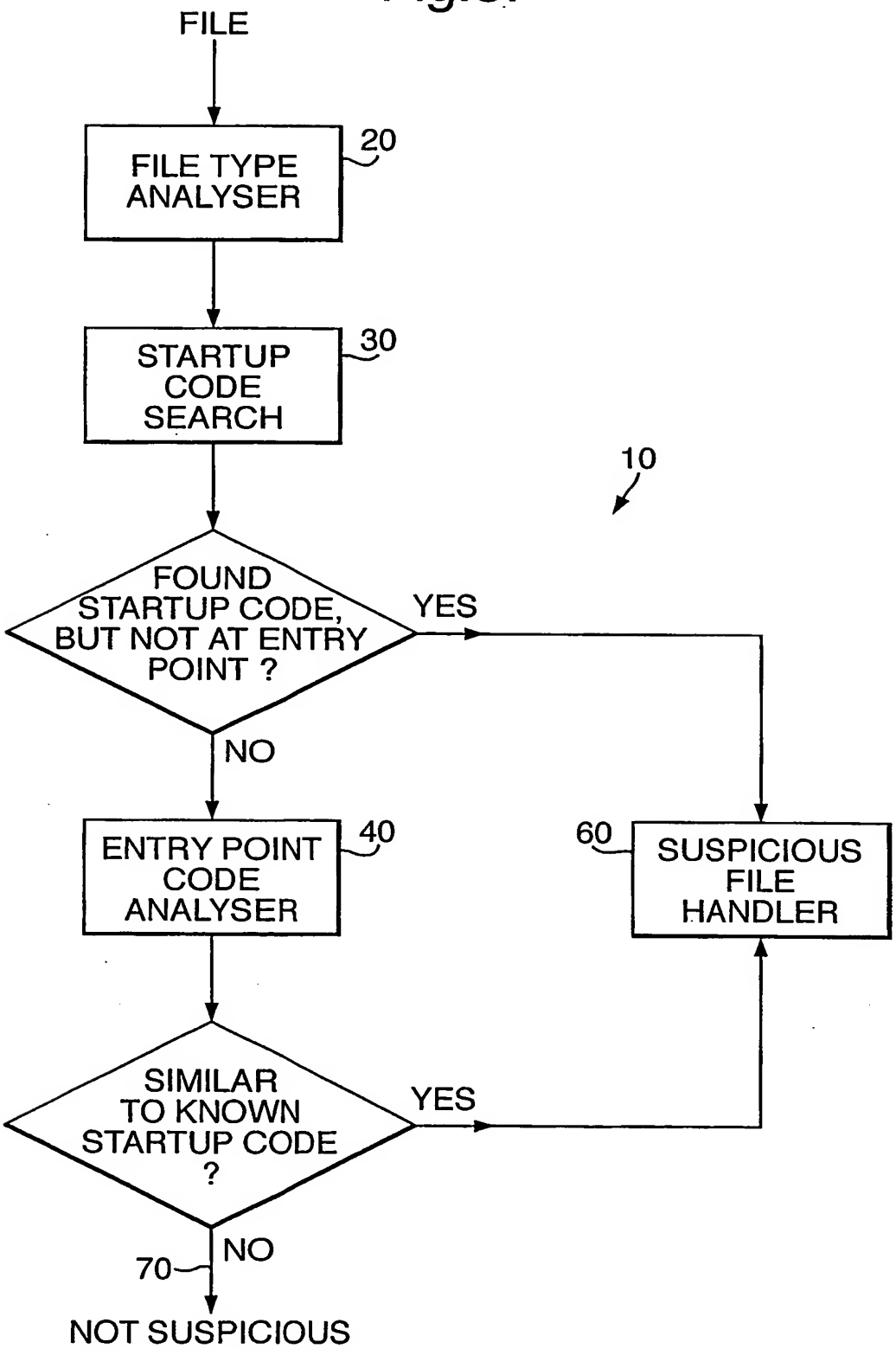


Fig.3.


FILE
FILE TYPE ANALYSER
20
STARTUP CODE SEARCH
30
10
FOUND STARTUP CODE, BUT NOT AT ENTRY POINT ?
YES
NO
ENTRY POINT CODE ANALYSER
40
60
SUSPICIOUS FILE HANDLER
SIMILAR TO KNOWN STARTUP CODE ?
YES
NO
70
NOT SUSPICIOUS